AMENDMENT TO CLAIMS

Please amend claims 1, 2, 33, 35, and 40, all as shown below. All pending claims are reproduced below, including those that remain unchanged. Claims 4-20 have been renumbered back to 33-49. Claims 4-32 were previously withdrawn.

1. (Currently amended) A machine system for protecting access constrained information from unauthorized access by way of unauthorized users or unauthorized programs, said machine system comprising:

(a) data-providing means for providing data of an identified one of two or more digital data files, where each of said files is identifiable by a file name and where each of said files is stored and retrievable ~~either locally or~~ remotely;

(b) an interceptable access mechanism through which data of an identified file of the data-providing means is accessed by identifiable, access-requesting programs and/or access-requesting users;

(c) access-control means coupled to intercept data access attempts made through said interceptable access mechanism,

(c.1) wherein the access-control means includes deny/approve means for testing the intercepted data access attempts and responsively denying or approving intelligible or other data access to the data of an identified subset of said files based on one or more of the identity of an access-attempting program, the time of the access attempt, the machine or location from which the access request originates and a user associated with the access request, and

(c.2) wherein the access-control means includes permissions control means for responding to permission rules associated with respective ones of identifiable subsets of said files; and

(d) localizing means for transparently and temporarily localizing external files and respective external permission rules of such external files for use by said access-control means.

2. (Currently amended) A machine-implemented method for protecting access constrained information from unauthorized access by way of unauthorized users or unauthorized programs, said machine-implemented method comprising:

(a) in response to a navigation-based request, providing data of an identified one of two or more digital data files, where each of said files is identified in the navigation-based request by a file name, file handle, or equivalent and where each of said files is stored and retrievable ~~either locally or~~ remotely;

(b) intercepting data access attempts made through an interceptable access mechanism, wherein:

(b.1) the interceptable access mechanism is one through which data of an identified file of the data-providing means is accessed by identifiable, access-requesting programs and/or access-requesting users;

(b.2) the interceptable access mechanism includes access-control means includes deny/approve means for testing the intercepted data access attempts and responsively denying or approving intelligible or other data access to the data of an identified subset of said files based on one or more of the identity of an access-attempting program, the time of the access attempt, the machine or location from which the access request originates and a user associated with the access request, and

(b.3) the access-control means includes permissions control means for responding to permission rules associated with respective ones of identifiable subsets of said files; and said method further comprises:

(c) in response to those of said navigation-based requests which request external files, transparently and temporarily localizing the external files and the respective external permission rules of such external files for use by said access-control means.

3. (Previously presented) The machine-implemented protecting method of Claim 2 wherein:

confidential information is kept consistently in encrypted format when the confidential information either resides within a remote file server or within easily removable media or when such confidential information is in-transit along an untrusted (not-secure) communications link;

said confidential information is exposed in plaintext form on an as-needed and as-authorized basis, essentially only when said confidential information resides within a local client that is conveniently viewable by one or more authorized users;

said plaintext exposure is allowed to occur only after an authorized user validates his or her authorization to access the information at the local client.

4. (Withdrawn) A software product having manufactured instructing signals for instructing an instructable machine to carry out a file characterizing and processing method including deciding how to respond to an access request for accessing data of an identified file, where the file is identified as primarily residing on a given media, the machine-implemented characterizing and processing method comprising:

(a) first determining if the identified file is an access-constrained one, and if not, allowing unconstrained access to the data of the identified file;

(b) second determining if the identified file is one covered by OTF recryption processing, and if not, allowing recryption-free access to the data of the identified file;

(c) third determining if the identified file is one covered by bubble protection processing, and if not, allowing bubble-free access to the data of the identified file;

(d) if the identified file is one covered by bubble protection and/or OTF recryption processing, fetching from the given, primary-residence media of the file, permission-control signals for use by the OTF recryption processing and/or bubble protection processing in determining whether to respectively grant decrypted access or any access to the data of the identified file;

(c) if the given, primary-residence media of the identified file is external to, or easily removable from a protective housing of said instructable machine, transparently and temporarily localizing within the protective housing, a copy of the permission-control signals and a copy of the identified file; and

(f) using the transparently and temporarily localized copies of the identified file and its permission-control signals in responding to local access requests generated from within the protective housing of the instructable machine.

5. (Withdrawn) The software product of Claim 4 wherein said permission-control signals are digitally-signed and consistently stored in a predefined directory of the primary-residence media of the file.

6. (Withdrawn) A machine-implemented method for responding to file-opening requests submitted to a local machine having local securing means for physically securing stored data, said method comprising:

(a) first determining if a file that is to-be-opened per a submitted request is a resident of a remote or easily-removable media and if so, whether such a locally-nonresident and requested file is logically associated with access-constraining rules (AC-rules also stored remotely or on easily-removable media; and

(b) if respective localized versions of the requested, locally-nonresident, and AC-associated file or of the file's logically-associated AC-rules are not already physically secured within the local securing means of the local machine, respectively and securely importing copies of the locally-nonresident file and/or of the file's locally-nonresident AC-rules into the local securing means of the local machine.

7. (Withdrawn) The machine-implemented method of Claim 6 wherein said securely importing step includes:

(b.1) conducting a digital signature check on a locally-nonresident AC-rules copy before allowing such a, being-imported AC-rules copy to be deemed as being securely-imported and locally-resident.

8. (Withdrawn) The machine-implemented method of Claim 7 wherein said securely importing step includes:

(b.2) conducting a digital signature check on a locally-nonresident and AC-associated file copy before allowing such a, being-imported file copy to be deemed as being securely-imported and locally-resident.

9. (Withdrawn) The machine-implemented method of Claim 8 wherein said step of securely importing a locally-nonresident and AC-associated file copy is characterized by:

(b.2a) causing the digital signature check to be carried out on a plaintext version of the file copy even where the imported file copy is encrypted.

10. (Withdrawn) The machine-implemented method of Claim 6 wherein said securely importing step is characterized by:

(b.1) not transmitting between the remote or easily-removable media and the local securing means, a plaintext version of confidential information represented by the locally-nonresident file while said copy of the file is being securely imported.

11. (Withdrawn) The machine-implemented method of Claim 6 wherein said securely importing step is characterized by:

(b.1) not creating in the local machine, a nonvolatile, plaintext version of confidential information represented by the locally-nonresident file while or after said copy of the file is securely imported.

12. (Withdrawn) The machine-implemented method of Claim 6 wherein said locally-nonresident and requested file and its logically associated AC-rules are consistently stored together on a same removable medium or in a same remote machine even as the primary residence of the locally-nonresident and requested file migrates from one place to another, and said first determining step includes:

(a.1) looking for the logically-associated AC-rules in a predefined folder of the primary residence place of the locally-nonresident and requested file.

13. (Withdrawn) The machine-implemented method of Claim 6 and further comprising:

(c) using the localized copies of the requested file and its AC-rules for carrying out file access operations, where said file access operations can include gaining bubble-protected access

to the data of the file copy and/or gaining intelligible access to the information of encrypted data, if any, withing the file copy, provided that authorization to do so is present.

14. (Withdrawn) The machine-implemented method of Claim 13 and further comprising:

(d) after local use of the localized copies of the requested file and its AC-rules is complete, deleting the local copies if they had not been modified, or otherwise de-localizing a modified version of the file copy if authorized and permitted modification had taken place, where said de-localizing includes sending the modified version (which may be appropriately encrypted prior to transmission) back to the remote or easily-removable media form which the original file was copied from or sending the modified version to a new place of primary residence.

15. (Withdrawn) The machine-implemented method of Claim 13 and further comprising:

(d) during local use of the localized copies of the requested file and its AC-rules, tracking the availability of the remote or easily-removable media that stores the locally-nonresident and requested file; and

(e) if said tracking indicates the remote or easily-removable media is unavailable or a link to a remote machine containing said remote or easily-removable media is down, refusing an access request to the file even though the localized copy is locally available, said refusal creating an illusion that the file being used is the external one rather than the localized copy.

16. (Withdrawn) A files management method for managing access-constrained files and data representing their corresponding access-constraining rules (AC-rules), said management method comprising:

(a) keeping said access-constrained files and the data of their respective, logically associated AC-rules consistently stored together on a same removable medium or in a same remote machine even as the place of primary residence of the access-constrained files migrates from one place to another.

17. (Withdrawn) The files management method of Claim 16 and further comprising:

(b) keeping said logically associated AC-rules consistently stored in a predefined folder of the primary residence place of the corresponding access-constrained files.

18. (Withdrawn) The files management method of Claim 16 and further comprising:

(b) providing a file-request handler at the primary residence place of the corresponding access-constrained files for keeping track of the logically associated AC-rules that correspond with specific ones or sets of the access-constrained files.

19. (Withdrawn) A software product having signals defining a file-use record, where the file-use record is for use in a local machine that can respond to file-opening requests submitted to the local machine, where the local machine has local securing means for physically securing stored data therein, including localized copies of non-resident files that reside primarily on remote or easily-removable media and are subject to access-control rules, and where the file-use record of said software product comprises at least one of:

(a) a channel status field for indicating whether a communications channel to the media of a corresponding, non-resident file is currently operative or not;

(b) a media availability status field for indicating whether the media of a corresponding, non-resident file is currently removed or not;

(c) a media locality field for indicating whether the media of a corresponding file is native or a not-permanently-resident one;

(d) a first section for keeping track of current, access-constraining states associated with the locally-native or temporarily localized file;

(e) a second section for keeping track of current usage by local application programs of the locally-native or temporarily localized file that is subject to access constraining; and

(f) a third section for keeping track of the primary residence location of the temporarily localized file.

20. (Withdrawn) A network system having a files management subsystem for managing localized access to access-constrained files where the access-constrained files each have a primary place of residence within the network and have corresponding access-constraining rules (AC-rules) defined by data stored at the corresponding primary place of residence of the respective files, said network system comprising:

(a) a plurality of file-servers and/or storage media units coupled to a network;

(b) at least one client coupled to the network for accessing file data of files stored on the file-servers and/or storage media units, where the at least one client includes:

(b.1) local securing means for physically securing stored data;

(b.2) importing means for securely importing copies of locally-nonresident file and/or of the file's locally-nonresident AC-rules into the local securing means of the client; and

(b.3) local constraining means for constraining access to data of locally-resident files and/or of imported local copies of said locally-nonresident files in accordance with corresponding locally-resident AC-rules and/or imported local copies of said locally-nonresident AC-rules.

21. (Withdrawn) The network system of Claim 20 wherein the at least one client includes:

(b.4) exporting means for securely exporting the data of locally-modified copies of locally-nonresident files to their corresponding primary places of residence within the network.

22. (Withdrawn) The network system of Claim 21 wherein the at least one client further includes:

(b.4a) export delay means for keeping track of how many local application programs, if any, are still reading or trying to further modify the locally-modified copies of locally-nonresident files, and for delaying said secured export of the data of the locally-modified copies even after a currently-modifying, local application program finishes using the locally-modified copies.

23. (Withdrawn) The network system of Claim 22 wherein said access-constraining rules include at least one of:

(d.1) OTF recryption rules;

(d.2) bi-directional Bubble-protection rules;

(d.3) uni-directional Bubble-protection rules (e.g., those that allow write-only access but not read-only access or vice versa); and

(d.4) user-ID based access-constraining rules.

24. (Withdrawn) The network system of Claim 20 wherein said access-constraining rules include at least one of:

(d.1) OTF recryption rules;

(d.2) bi-directional Bubble-protection rules;

(d.3) uni-directional Bubble-protection rules (e.g., those that allow write-only access but not read-only access or vice versa); and

(d.4) user-ID based access-constraining rules.

25. (Withdrawn) The network system of Claim 20 wherein said files management subsystem includes:

(c) migration control means for keeping said access-constrained files and the data of their respective, logically associated AC-rules consistently stored together on a same removable medium or in a same server even as the place of primary residence of the access-constrained files migrates from one place to another.

26. (Withdrawn) A client machine for use in a network system having files defined as access-constrained files where the access-constrained files each have a primary place of residence within the network and have corresponding access-constraining rules (AC-rules) defined by data stored at the corresponding primary place of residence of the respective files, said client machine comprising:

(a) importing means for securely importing copies of locally-nonresident files and/or of the files' locally-nonresident AC-rules from the network and into the client machine; and

(b) local constraining means for constraining access to data of locally-resident files and/or of imported local copies of said locally-nonresident files in accordance with corresponding locally-resident AC-rules and/or imported local copies of said locally-nonresident AC-rules.

27. (Withdrawn) The client machine of Claim 26 wherein said local constraining means includes:

(b.1) a decryption unit for providing intelligible access to information of encrypted ones of said access-constrained files;

(b.2) flow-blocking switches for blocking the flow of file data either directly to a requesting application program or indirectly by way of said decryption unit to the requesting application program;

(b.3) a permissions control module that controls said flow-blocking switches to thereby block all access by the requesting application program to the requested file data, or to block intelligible access to information of encrypted portions, if any, of the requested file data, or to grant nondecrypted access to the data of the requested file data, or to grant intelligible access to the encrypted portions, if any, of the requested file data;

(b.4) a local and physically-secured permission-rules storing memory that stores local AC-rules and/or copies of securely imported ones of locally-nonresident AC-rules, where the stored AC-rules are usable for governing the actions of the permissions control module.

28. (Withdrawn) The client machine of Claim 26 wherein said AC-rules can govern the actions of the permissions control module on the basis of at least one or more of:

(b.4a) temporally based constraints regarding the time that access is requested to a corresponding, access-constrained file;

(b.4b) geographically based constraints regarding the location from which a request is generated for access to a corresponding, access-constrained file;

(b.4c) machine identification based constraints regarding the unique identification of the machine from which a request issued for access to a corresponding, access-constrained file;

(b.4d) program identification based constraints regarding the unique identification of the executing program or programs whose actions led to a request being issued for access to a corresponding, access-constrained file;

(b.4e) user identification based constraints regarding the unique identification of one or more human users whose recent actions led to a request being issued for access to a corresponding, access-constrained file; and

(b.4f) navigation-path based constraints regarding the unique way in which a path was navigated to point to the access-constrained file for which a request was issued for access to corresponding file data.

29. (Withdrawn) The client machine of Claim 26 and further comprising:

(c) a ubiquitous navigating mechanism for seamlessly pointing to external files stored on the network or on externalizable media, as easily as for pointing to locally stored files so that a novice user can be left unaware of what is the primary place of residence of a pointed-to file.

30. (Withdrawn) The client machine of Claim 26 wherein said local constraining means includes:

(b.1) volatile storage means for temporarily storing plaintext data derived from a selected one the two or more digital data files; and

(b.2) volume-encryption means for decrypting confidential data portions of a selected one of said access-constrained, digital data files and for transmitting the decrypted confidential data to the volatile storage means after local approval for such intelligible access is locally granted.

31. (Withdrawn) The client machine of Claim 26 wherein said local constraining means includes:

(b.1) bubble-control means which intercepts file-OPEN requests made by identifiable, requesting programs for access to data of an access-constrained file and determines whether or

not to approve access to the data of the file based on at least one of the following, user-ID independent factors:

(b.1a) identity of the requesting application program;

(b.1b) when the file-OPEN request is made;

(b.1c) location from where the file-OPEN request is made;

(b.1d) unique identity of the client machine such as serial number; and

(b.1e) whether the request is a unidirectional, read-only or write-only type of request..

32. (Withdrawn) The client machine of Claim 31 wherein:

(b.1f) the bubble-control means posts a security alert message to the network upon denial of a file-OPEN request by the bubble-control means.

433. (Currently amended) An instruction conveying means for instructing an instructable machine to carry out an access-constraining method for files that ~~primarily~~ reside either inside or outside the instructable machine, where the instructable machine has an internal, data-providing means that can provide data from an identified one of internal or external, plural digital data files in response to interceptable file-access requests, where each of said files is identifiable by a file name, said machine-implemented, access-constraining method being for protecting data and/or information of said files from unauthorized access by way of unauthorized ones of identifiable programs and/or at the behest of unauthorized, identifiable users, said internal/external access-constraining method comprising:

(a) intercepting data access attempts made by access requesting programs for data in an identified one of files residing ~~primarily~~ on an identified internal, removable, or external media;

(b) first testing for each intercepted data access attempt, to verify that the identified media on which the requested file ~~primarily~~ resides is currently available, and if not, updating local records which track the current availability of the identified media to indicate the current non-availability of the media;

(c) second testing for each intercepted data access attempt, to determine if access constraining control information is already available internally for the identified file;

(d) if said second testing shows that the access constraining control information is not available in an internal and physically-secure storage area, attempting to securely import the missing, access constraining control information from the removable, or external media of primary residence of the identified file;

(e) if said import attempt shows that the missing, access constraining control information is unavailable, determining explicitly or implicitly if the missing information is necessary for allowing the intercepted access-request to complete normally to provide a grant of the request, and if the missing information is necessary, blocking the intercepted access-request from completing normally and thereby blocking the provision of said grant in response to the intercepted access-request.

~~5~~34. (Original) The instructions conveying means of Claim 33 and further wherein said step (d) of attempting to securely import the missing, access constraining control information includes at least one of:

(d.1) verifying a digital signature covering corresponding access constraining control information that is held in said removable, or external media of primary residence of the identified file and imported into said instructable machine;

(d.2) decrypting imported digital data that represents the corresponding access constraining control information of the identified file; and

(d.3) storing a digital-signature authenticated and/or decrypted, plaintext version of the missing, access constraining control information in said internal and physically-secure storage area of the instructable machine.

~~6~~35. (Currently amended) The instructions conveying means of Claim 33 and wherein said internal/external access-constraining method further comprises:

(f) third testing for each intercepted data access attempt, to determine if the identified file is an access constrained one which resides ~~primarily~~ on removable, or external media, and if so to determine whether a localized copy of the identified file is present in the instructable machine;

(g) if said third testing shows that the localized copy is not present, importing a copy of the identified file into said internal and physically-secure storage area of the instructable machine.

~~7~~36. (Original) The instructions conveying means of Claim 35 and wherein said internal/external access-constraining method further comprises:

(h) recording the time of said importing of the copy of the identified file so that said time of localization can be later used by garbage collection mechanisms of the instructable machine to remove localized copies that have remained localized beyond a predefined time limit.

~~8~~37. (Original) The instructions conveying means of Claim 35 and wherein said internal/external access-constraining method further comprises:

(h) determining if the just-localized file copy imported in step (g) is one whose primary data is encrypted;

(i) attempting to decrypt the encrypted primary data of the just-localized file copy if the determining step (h) shows that such encrypted data is present; and

(j) blocking the intercepted access-request from completing normally and thereby blocking the provision of said grant in response to the intercepted access-request if the attempted decryption of step (i) is unsuccessful.

~~9~~38. (Original) The instructions conveying means of Claim 37 and wherein said internal/external access-constraining method further comprises:

(k) attempting to verify a digital signature covering the decrypted primary data of step (i); and

(l) blocking the intercepted access-request from completing normally and thereby blocking the provision of said grant in response to the intercepted access-request if the signature verification of step (k) is unsuccessful.

~~10~~39. (Original) The instructions conveying means of Claim 37 and wherein said internal/external access-constraining method further comprises:

(k) volume encrypting the decrypted primary data of step (i) and storing the volume encrypted data to nonvolatile storage;

wherein the decrypted primary data is kept within the instructable machine exclusively in volatile storage thereof.

~~1140~~. (Currently amended) An instructions conveying means for instructing an instructable machine to carry out an nonresident file-closing method for files that ~~primarily~~ reside removably or outside the instructable machine, where the instructable machine has an internal, data-providing means that can provide data from an identified one of internal or external, plural digital data files in response to interceptable file-open requests, where each of said files is identifiable by a file name, said machine-implemented, file-closing method being for protecting data and/or information of said nonresident files from unauthorized access by way of unauthorized ones of identifiable programs and/or at the behest of unauthorized, identifiable users, said nonresident file-closing method comprising:

(a) intercepting file-closing attempts made by access-completing parts of access-requesting programs, where the original access requests were for data in an identified one of files residing ~~primarily~~ on an identified internal, removable, or external media;

(b) first testing for each intercepted file-closing attempt, to verify that the identified media on which the to-be-closed file ~~primarily~~ resides is currently available, and if not, updating local records which track the current availability of the identified media to indicate the current non-availability of the media;

(c) second testing for each intercepted file-closing attempt, to determine if access constraining control information is available internally for the identified file;

(d) if said second testing shows that the access constraining control information is not available in an internal and physically-secure storage area, determining explicitly or implicitly if the missing, access constraining control information must be locally present for allowing the intercepted file-closing request to complete normally, and if the missing information is necessary, blocking the intercepted file-closing request from completing normally in response to the intercepted file-closing request.

~~12~~41. (Original) The instructions conveying means of Claim 40 and wherein said nonresident file-closing method further comprises:

(e) third testing the locally-present, access constraining control information for the to-be-closed file to determine if the access constraining rules for the identified file permit a current attempt to close the file; and

(f) blocking the intercepted file-closing request from completing normally if said third testing step (e) indicates the locally-present, access constraining control information for the to-be-closed file do not permit a current attempt to close the file.

~~13~~42. (Original) The instructions conveying means of Claim 41 and wherein said nonresident file-closing method further comprises:

(g) determining if other local, application programs are still using the localized file copy, and if so, fooling the file-closing requesting application program into to thinking the nonresident original of the identified file bas been closed, even though said nonresident original has not yet been closed.

~~14~~43. (Original) The instructions conveying means of Claim 42 and wherein the nonresident file-closing method further comprises:

(h) if no other local, application programs are still using the localized file copy, determining if the localized file copy has been modified locally; and

(i) if said determining step (h) shows that the localized file copy has not been modified locally, allowing the intercepted file-closing request to complete normally, thereby causing a file-close action to occur for the nonresident file identified in a counterpart, file-opening request.

~~15~~44. (Original) The instructions conveying means of Claim 43 and wherein the nonresident file-closing method further comprises:

(j) in conjunction with said step (i) of allowing the requested file-close action to occur for the nonresident file, deleting the localized file copy.

~~1645~~. (Original) The instructions conveying means of Claim 44 and wherein the nonresident file-closing method further comprises:

(k) in conjunction with said step (i) of allowing the requested file-close action to occur for the nonresident file, determining if any other, temporarily localized filed copies (TTL'ed files) are logically associated with the localized copy of the access constraining rules of the to-be-closed file, and if not, deleting the localized copy of the access constraining rules of the to-be-closed file.

~~1746~~. (Original) The instructions conveying means of Claim 43 and wherein the nonresident file-closing method further comprises:

(j) if said determining step (h) shows that the localized file copy has been modified locally, overwriting the modified local copy to the nonresident, original location before allowing the intercepted file-closing request to complete normally, thereby causing a file-close action to occur for the nonresident file identified in a counterpart, file-opening request only after the nonresident file has been updated in accordance with the locally-made modifications.

~~1847~~. (Original) The instructions conveying means of Claim 41 and wherein the nonresident file-closing method further comprises:

(e) in response to a denial of the requested file-closing, posting a correspondingly security alert message.

~~1948~~. (Original) In an automated machine for executing one or more application programs, where the application programs access file data of a plurality of locally and externally stored files by causing interceptable file-OPEN requests and file-CLOSE requests to be sent to an operating system of said machine, and where data within a subset of the plurality of stored files is encrypted or otherwise access constrained; an automatic access constraining control mechanism comprising:

(a) OPEN intercept means for intercepting said interceptable file-OPEN requests;

(b) selective OPEN continuance means, responsive to the OPEN intercept means, for determining whether an intercepted file-OPEN request is requesting an open of a file for which the request is to be denied based on associated access constrain rules;

(c) local-use tracking means , responsive to the selective OPEN continuance means, for determining whether a localized copy of a to-be-opened, nonresident file, and a localized copy of nonresident access constraining rules associated with the to-be-opened, nonresident file, are already present in the machine, and if so, for allowing the intercepted file-OPEN request to continue on its way to the operating system such that the localized file copy will be accessed if so permitted by the localized copy of nonresident access constraining rules;

(d) CLOSE intercept means for intercepting said interceptable file-CLOSE requests; and

(e) selective CLOSE continuance means, responsive to the OPEN intercept means, for determining whether an intercepted file-CLOSE request is requesting a closing of a file for which the CLOSE request is to be denied based on associated access constrain rules.

~~2049~~. (Original) The instructions conveying means of Claim 41 and wherein said nonresident file-closing method further comprises:

(g) determining if the to-be-closed file is a special-use one such that, even if there are no other local, application programs still using the localized file copy, still fooling the file-closing requesting application program into to thinking the nonresident original of the identified file has been closed, even though said nonresident original has not yet been closed because it is later slated for special-use by an application program that has not yet started using the localized file copy.